ABSTRACT OF THE DISCLOSURE

Outgoing data units, such as packets, from a computer system that contain data characteristic of an operating system executing on the computer system are intercepted before they are transmitted on a network and masked to impersonate a different operating system if the network is untrusted. The masking may be to re-fingerprint the data units by replacing the data characteristic of the actual operating system with data characteristic of the different operating system. Alternatively, the masking may require discarding the data unit and not transmitting it. In another aspect, certain incoming packets are also intercepted and a false response that is characteristic of the different operating system is sent to mask the actual operating system. The appropriate masking is specified by a security policy that identifies untrusted networks, the types of data units to be masked, the action to be taken to mask the data units, and re-fingerprinting data to be used as replacement data.